Symantec AntiSpam™ for SMTP Implementation Guide

symantec™

Symantec AntiSpam™ for SMTP Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 3.1.0

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introducing Symantec AntiSpam for SMTP

About Symantec AntiSpam for SMTP 7
How Symantec AntiSpam for SMTP works 8

Chapter 2 Installing Symantec AntiSpam for SMTP

Before you install 9
Installing and configuring the operating system 10
Configuring DNS 10
Preventing conflicts with other SMTP servers 11
System requirements 11
Installing Symantec AntiSpam for SMTP 12
Verifying DNS on the Symantec AntiSpam for SMTP server 13
Running the installation script or setup program 14
Specifying locations for installation directories 15
Selecting an HTTP server port 17
Selecting an HTTPS server port 17
Post-installation tasks 18
Accessing the administrative interface 18
Routing processed email for delivery 19
Stopping and restarting Symantec AntiSpam for SMTP 20
Uninstalling Symantec AntiSpam for SMTP 20

Chapter 3 Configuring Symantec AntiSpam for SMTP

Configuring administrator settings 23
Configuring connection and delivery options 27
Configuring SMTP options 27
Configuring delivery options 28
Configuring HTTP options 29
Configuring HTTPS options 30
Processing messages in the hold queue 33
Configuring routing options 34
Configuring default routing 34
Configuring local routing 36
Configuring alerts 39
Configuring logging options 41

Configuring diagnostic settings 43
- Configuring queue file save 44
- Configuring SMTP conversation logging 45

Chapter 4 Setting your blocking policy

About your blocking policy 47
Blocking by message criteria 48
- Blocking by message size 48
- Blocking by subject line 49

Blocking spam 49
- Blocking by a sender’s email address 50
- Blocking by DNSBL anti-spam lists 51
- Excluding by anti-spam white lists 53
- Identify suspected spam messages by the heuristic spam engine 54

Preventing spam relaying 55
- Configuring external relay restrictions 55
- Blocking by characters in email addresses 57

Chapter 5 Notifications, logging, and reporting

About the Status page 59
About notifications 61
- Understanding sender notifications 61
- Understanding administrator notifications 61
- Understanding notification metatags 62
- Configuring notifications 63

Generating reports 63
- Generating summary reports 64
- Generating detail reports 65

Chapter 6 Integrating Symantec AntiSpam for SMTP with SESA

About SESA 69
Configuring logging to SESA 70
- Configuring SESA to recognize Symantec AntiSpam for SMTP 71
- Installing the local SESA Agent using the Agent Installer 72
- Installing the SESA Agent manually by command line 76
- Configuring Symantec AntiSpam for SMTP to log events to SESA 77

Interpreting Symantec AntiSpam for SMTP events in SESA 78
Uninstalling the SESA Integration Package 78
Uninstalling the local SESA Agent 79

Introducing Symantec AntiSpam for SMTP

This chapter includes the following topics:

- About Symantec AntiSpam for SMTP
- How Symantec AntiSpam for SMTP works

About Symantec AntiSpam for SMTP

Symantec AntiSpam for SMTP is a Simple Mail Transfer Protocol (SMTP) server that processes email before sending it to a local mail server for delivery. You configure the software through the administrative interface, from either the physical server on which Symantec AntiSpam for SMTP is installed or from any workstation on the network. Symantec AntiSpam for SMTP can be configured to block messages based on the following:

- Message size
- Subject line
- Sender address
- Domain Name Server Black List (DNSBL) anti-spam lists
- Heuristic spam detection (in conjunction with subject blocking)
- Anti-relay settings
- Characters in email address

You can configure Symantec AntiSpam for SMTP so that users on the network become aware of its operation only if a content or spam list violation is detected. You can also configure Symantec AntiSpam for SMTP to send alerts to administrators in the case of system events.

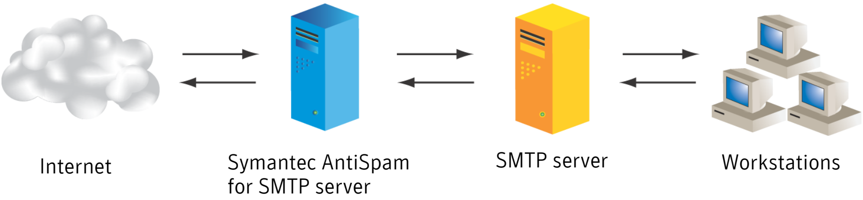
See "Configuring alerts" on page 39.

How Symantec AntiSpam for SMTP works

In a typical configuration, Symantec AntiSpam for SMTP operates as an SMTP server that accepts incoming email from the Internet, processes the email based on the configuration of the product, and delivers the email to another SMTP server for delivery. It also receives outgoing email from your SMTP server and processes it based on the configuration of Symantec AntiSpam for SMTP.

Figure 1-1 shows how Symantec AntiSpam for SMTP is typically configured on a network.

Figure 1-1 Typical processing path: Symantec AntiSpam for SMTP



When Symantec AntiSpam for SMTP receives an email message, it sends the message to the fast queue (a logical queue with a large number of dedicated threads) to be processed. During processing, Symantec AntiSpam for SMTP can block messages by message size, subject line, sender address, a DNSBL anti-spam list, and characters in email addresses. Messages identified by the heuristic spam engine prepend text to the subject line (for example, Spam:), and the messages are delivered.

If a message cannot be delivered, it is forwarded to the slow queue so as not to backlog the fast queue. Once a message is in the slow queue, Symantec AntiSpam for SMTP continues to attempt delivery of the message. Symantec AntiSpam for SMTP reorders messages in the slow queue, moving messages that will not deliver to the rear of the queue, and moving to the front of the queue messages destined to the same host on the next hop (if those hosts are accepting delivery). If a message is not able to be delivered within the specified number of days, the forwarding server returns a reason (wrong domain, user name doesn't exist, for example), and the file is deleted from the slow queue.

Chapter 2

Installing Symantec AntiSpam for SMTP

This chapter includes the following topics:

- Before you install
- System requirements
- Installing Symantec AntiSpam for SMTP
- Post-installation tasks
- Uninstalling Symantec AntiSpam for SMTP

Before you install

You must perform the following pre-installation tasks when appropriate:

- Install and configure the operating system.
  See "Installing and configuring the operating system" on page 10.
- Configure DNS.
  See "Configuring DNS" on page 10.
- Prevent conflicts with other SMTP servers.
  See "Preventing conflicts with other SMTP servers" on page 11.

Installing and configuring the operating system

Your server's operating system software and applicable updates must be installed, configured, and working correctly before you install Symantec AntiSpam for SMTP. Consult your server's documentation for more information. Installation of your operating system software and updates is outside the scope of this guide.

Configuring DNS

Symantec AntiSpam for SMTP works in conjunction with other SMTP mail servers. By properly configuring your site's DNS, email that is destined for your existing mail server arrives at Symantec AntiSpam for SMTP first. After processing email, Symantec AntiSpam for SMTP forwards messages to your SMTP server for delivery.

The DNS zone for your site must be configured to support reverse name lookup, which is used to verify the IP address of the host or domain that you are trying to resolve.

Symantec AntiSpam for SMTP processing is affected when you modify DNS records. There are two types of records that are involved in the delivery of email:

- A record: A mapping of host name to IP address. For example, the host name www.somewhere.com might map to the specific IP address 192.168.23.10.
- MX record: A mapping of domains to mail exchange host names. Any email that is sent to a particular user at a domain (such as user@somewhere.com) is resolved by a DNS server MX record to a host name, such as mailer.somewhere.com. Then, the A record resolves the name mailer.somewhere.com to an IP address.

By adding a higher priority MX record for the Symantec AntiSpam for SMTP host, all email that is destined for the mail server arrives at Symantec AntiSpam for SMTP first. After processing, Symantec AntiSpam for SMTP forwards the email to the mail server for delivery.

Consult with your network administrator or Internet service provider (ISP) if you are unsure of how to configure DNS records.

Note: You may also choose to modify DNS so that the MX record points to the firewall, in which case, the firewall would route traffic internally. In this scenario, changes are made to the firewall rather than to the MX record.

Preventing conflicts with other SMTP servers

Because Symantec AntiSpam for SMTP is an SMTP server, it must have exclusive access to the TCP/IP port that corresponds to that service. No other SMTP servers can be running on the same port on the same server on which Symantec AntiSpam for SMTP is installed. You must disable these conflicting services prior to installing Symantec AntiSpam for SMTP.

Note: When you install Symantec AntiSpam for SMTP on a Solaris™ server, the installation program may detect conflicting programs that are commonly found on Solaris (such as the Solaris Sendmail™ program being run on port 25). If such programs are detected, the installation program will issue a warning and offer to disable these programs automatically. Although reasonable effort has been made to make the automatic disabling of these conflicting programs safe, the attempt may still fail, possibly leaving your server in an uncertain condition. Therefore, you may want to disable the conflicting programs prior to installing Symantec AntiSpam for SMTP.

System requirements

You need root or administrator-level privileges to install Symantec AntiSpam for SMTP. You should install Symantec AntiSpam for SMTP on its own server.

The minimum system requirements for Solaris and Windows NT/2000 Server are as follows:

- Solaris: SPARC®-based server
  Windows NT/2000 Server: Intel® Pentium® or compatible
- Solaris version 7.0 or 8.0
  Windows NT 4.0 with Service Pack 3 or later, or Windows 2000 Server with Service Pack 2
- 256 MB RAM (512 MB or more recommended for optimal performance)
- 50 MB to install (500 MB minimum after installation for email processing)
- Static IP address for the computer that will run Symantec AntiSpam for SMTP
- TCP/IP Internet connection
- Appropriately configured DNS, to include Address (A), Pointer (PTR), and Mail eXchange (MX) records for your servers

- DNS zone for your site that is configured to support reverse name lookup
- Netscape Navigator version 4.75 or later, or Microsoft Internet Explorer version 5.0 or later

Installing Symantec AntiSpam for SMTP

Note: You should install Symantec AntiSpam for SMTP on a separate server from your SMTP server so that there is no significant impact on network resources.

You need root or administrator-level privileges to install Symantec AntiSpam for SMTP. A static IP address is required.

If you decide to install Symantec AntiSpam for SMTP on the same computer as your SMTP server, you must configure Symantec AntiSpam for SMTP to listen on a port other than the one on which your SMTP server listens. Because port 25 is the port to which most servers send email connection requests, you will most likely want to have Symantec AntiSpam for SMTP listen on port 25. If your SMTP server is currently listening on port 25, you must change your server to listen on a different port.

On Solaris, if another process is running on port 25, Symantec AntiSpam for SMTP attempts to automatically disable it. A record that the process has been disabled is placed in the log directory. If another process is disabled because it is running on port 25, there is an on-screen option during installation that lets you stop the installation process and change the port for the existing process or allow Symantec AntiSpam for SMTP to disable the process and continue the installation on port 25.

Note: If another process that is running on port 25 is disabled, you must configure the disabled software to run on another port.

Complete the following tasks in the order in which they are listed to install Symantec AntiSpam for SMTP:

- Verify that DNS is properly configured for your network.
  See “Verifying DNS on the Symantec AntiSpam for SMTP server” on page 13.
- Run the installation script or setup program to install.
  See “Running the installation script or setup program” on page 14.

- Specify the locations for the installation directories.
  See "Specifying locations for installation directories" on page 15.
- Select an HTTP server port.
  See "Selecting an HTTP server port" on page 17.
- Select an HTTPS server port.
  See "Selecting an HTTPS server port" on page 17.

Verifying DNS on the Symantec AntiSpam for SMTP server

Your server must be configured as a DNS client prior to installing Symantec AntiSpam for SMTP.

Verify and test your DNS settings

To verify your DNS settings, you must check your TCP/IP properties. To test your DNS server, use the Name Server Lookup (nslookup) utility.

To verify your DNS settings on Windows 2000 Server

1. Open Local Area Connection Properties.
2. Click **Internet Protocol (TCP/IP)**.
3. Click **Properties**.
4. Click **Advanced**.
5. On the DNS tab, specify the domain suffix and verify that at least one valid DNS server is listed in the DNS server addresses list.
   The host name is the computer name that is entered in System Properties on the Network Identification tab.

Consult with your network administrator or Internet service provider (ISP) if you are unsure of the values to use.

To verify your DNS settings on Windows NT

1. Open the Network control panel.
2. On the Protocols tab, click **TCP/IP Protocol**.
3. Click **Properties**.
4. In the TCP/IP Properties window, click **DNS**.
5. Verify that the Host Name and Domain boxes contain the correct values and that at least one valid DNS server is listed in the DNS Service Search Order list.

To verify your DNS settings on Solaris

1. Open the following file:
   /etc/resolv.conf
   The file should contain lines similar to the following:
   domain somewhere.com
   nameserver 192.168.1.2
   nameserver 192.168.9.7
   Verify that the specific domain name and name server addresses that are used in your file are correct for your site.
   Consult with your network administrator or Internet service provider (ISP) if you are unsure of the values to use.
2. Make any necessary changes.

If the /etc/resolv.conf file does not exist on your server, create it using the above example as a template. Replace the domain name and name server addresses with values that are correct for your site.

To test your DNS server

◆ Run the NSLookup command in the following format:
nslookup <IP address or server name>
For example, nslookup 155.55.55.55

The IP address should resolve to your server name, and the server name should resolve to your IP address.

Note: You should run NSLookup twice (once in the format “nslookup <host name>” and once as “nslookup <IP address>”).

Running the installation script or setup program

You must run the installation script (Solaris) or setup program (Windows NT/2000 Server) to install Symantec AntiSpam for SMTP.

Run the installation script or setup program

For Solaris, you must be logged on as root. The Symantec AntiSpam for SMTP files are on the CD.

For Windows NT/2000 Server, you must be logged on with administrator privileges. The Symantec AntiSpam for SMTP files are on the CD.

To install Symantec AntiSpam for SMTP on Solaris

1. Change (cd) to the location of the installation files.
2. Type the following command to run the installation script:
   sh sassmtp.sh
3. Follow the on-screen directions.
   A transcript of the installation is saved as /var/log/SASSMTP-install.log for later review, if necessary.
4. Verify that the software is running by viewing the Status page.
   The Date server started field should be current.
   See "About the Status page" on page 59.

To install Symantec AntiSpam for SMTP on Windows NT/2000 Server

1. Change (cd) to the location of the installation files.
2. Run Setup.exe.
3. Follow the on-screen directions.
4. Verify that the software is running by viewing the Status page.
   The Date server started field should be current.
   See "About the Status page" on page 59.

Specifying locations for installation directories

Symantec AntiSpam for SMTP is organized into directories that each contain specific kinds of files.

The location of each directory can be specified during installation, during which a default location is shown. Unless you have a compelling reason to do otherwise, you should accept the default location.

Table 2-1 shows the default installation directory locations for Solaris.

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
InstallDir	Contains the Symantec AntiSpam for SMTP program files and read-only data files. At least 5 MB disk space required.	/opt/SASSMTP
MailDir	Contains SMTP queue files. At least 500 MB disk space recommended.	/var/opt/SASSMTP/queues

Table 2-1 Installation directories for Solaris

Directory	Description	Default location
LocalDir	Contains server-specific configuration files. At least 1 MB disk space required.	/var/opt/SASSMTP/local
LogDir	Contains log files that record Symantec AntiSpam for SMTP activity. At least 600 MB disk space recommended.	/var/opt/SASSMTP/logs
DiagDir	Contains files that may help Symantec technicians address issues that may arise with the software. At least 34 MB disk space recommended.	/var/opt/SASSMTP/queues/diagnosticfiles
DocsDir	Contains readme. At least 1 MB disk space recommended.	/opt/SASSMTP/manuals/english

Table 2-2 shows the Windows default installation directory locations.

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Install	Contains the Symantec AntiSpam for SMTP program files and read-only data files. At least 5 MB disk space required.	\ProgramFiles\Symantec\SASSMTP
Queues	Contains SMTP queue files. At least 500 MB disk space recommended.	\ProgramFiles\Symantec\SASSMTP\queues
Local	Contains server-specific configuration files. At least 1 MB disk space required.	\ProgramFiles\Symantec\SASSMTP\local
Logs	Contains log files that record Symantec AntiSpam for SMTP activity. At least 600 MB disk space recommended.	\ProgramFiles\Symantec\SASSMTP\logs

Table 2-2 Installation directories for Windows

Directory	Description	Default location
Diagnostic	Contains files that may help Symantec technicians address issues that may arise with the software. At least 34 MB disk space recommended.	\ProgramFiles\Symantec \SASSMTP\queues\diagnostic files
Docs	Contains readme. At least 1 MB disk space recommended.	\Program Files\Symantec\SASSMTP\ docs\english

Selecting an HTTP server port

The Symantec AntiSpam for SMTP software is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with Symantec AntiSpam for SMTP. This HTTP server is independent of any existing HTTP server that already may be installed on your server and is not a general-purpose Web server.

During the installation process, you will be prompted for the TCP/IP port number on which this built-in HTTP server will listen. The number that you specify becomes the port number in the URLs you will use to access the Symantec AntiSpam for SMTP interface. The port number that is specified must be different from the HTTPS and SMTP port numbers, exclusive to Symantec AntiSpam for SMTP, and not already in use by any other program or service.

Because the built-in HTTP server is not a general-purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). Unless you have a compelling reason to do otherwise, you should use the default port number of 8003. If you select a port number other than the default, do not forget which port number you selected.

Selecting an HTTPS server port

HTTPS stands for HTTP via Secure Sockets Layer (SSL). With HTTP, all information is sent in clear text with no authentication between client and server. With HTTPS, there is client and server authentication via a certificate that has been signed by a Certificate Authority. Once a legitimate Web certificate is installed on Symantec AntiSpam for SMTP, the server and client now share a common key that lets them encrypt and decrypt messages that they send to each other. In Symantec AntiSpam for SMTP, secure connections are used for the logon- and password-changing portions of the administrative interface when they are enabled.

During installation, you must identify the TCP/IP port number on which the HTTPS server will listen. The port number that you specify must be different from the HTTP and SMTP port numbers, exclusive to Symantec AntiSpam for SMTP, and not already in use by any other program or service. The default HTTPS port number is 8043. Unless you have a compelling reason to do otherwise, you should select the default.

Note: You must identify an HTTPS port number during installation even if you do not enable SSL.

Post-installation tasks

You must perform the following post-installation tasks when appropriate:

- Access the administrative interface.
  See "Accessing the administrative interface" on page 18.
- Route scanned email for delivery.
  See "Routing processed email for delivery" on page 19.
- Stop and restart Symantec AntiSpam for SMTP.
  See "Stopping and restarting Symantec AntiSpam for SMTP" on page 20.

Accessing the administrative interface

You must access the administrative interface to configure Symantec AntiSpam for SMTP.

Access the Symantec AntiSpam for SMTP administrative interface

You can access Symantec AntiSpam for SMTP through a browser window, from the Start menu, or by clicking the desktop icon (if it is running on Windows).

To access the Symantec AntiSpam for SMTP administrative interface via a browser window

1. Open your browser.
2. Type the Symantec AntiSpam for SMTP IP address or host name in the following format:
   http://<IP address or host name of the computer that is running the software>:<port #>
   For example, use either of these formats:
   http://savsmtp.somewhere.com:8003
   http://198.0.0.1:8003

3 Log on using the password that you set during installation.

Passwords are case sensitive.

To access the Symantec AntiSpam for SMTP administrative interface via the Start menu

1 On the Windows taskbar, click **Start** > **Programs**.

2 Click **Symantec AntiSpam for SMTP**.

Routing processed email for delivery

Unless the Symantec AntiSpam for SMTP server is the last hop before the Internet, you must configure Symantec AntiSpam for SMTP to route processed email to your mail hosts for delivery.

To route processed email for delivery

1 Open Symantec AntiSpam for SMTP.

2 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

3 On the Routing tab, under Local Routing List, click **Add**.

4 Under Routing list entry, in the Host or Domain box, type the domain of your mail server (for example, brightcorp.com).

5 Under Destination relay, in the Host box, type the fully qualified domain name or IP address of your mail server.

6 In the Port box, type the port number of your mail server.

7 Click **Save**.

Note: You must add a routing list entry for each serviced email domain on your network.

All mail that was previously destined for your SMTP server goes to Symantec AntiSpam for SMTP for processing, then is forwarded to your SMTP server for delivery.

Stopping and restarting Symantec AntiSpam for SMTP

You may need to stop and restart Symantec AntiSpam for SMTP. Stopping and restarting the service results in a lost connection to client applications that may be submitting a file for processing or delivery. The client application must reestablish the connection and resubmit the file for processing and delivery.

If messages are being processed when the service is stopped, the processing of those messages stops. Messages are reprocessed when the service is restarted.

Stop and restart Symantec AntiSpam for SMTP

Instructions for stopping and restarting Symantec AntiSpam for SMTP differ depending on the operating system that you are running. If you are running Symantec AntiSpam for SMTP on Windows NT/2000 Server, stop and restart the service in the Services Control Panel.

To stop and restart Symantec AntiSpam for SMTP on Solaris

1. Stop the service by typing the following
   /etc/rc2.d/S87sassmtp stop
2. Restart the service by typing the following
   /etc/rc2.d/S87sassmtp start

To stop and restart Symantec AntiSpam for SMTP on Windows

1. On the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Services**.
2. Right-click **Symantec AntiSpam for SMTP**, then click **Stop**.
3. Right-click **Symantec AntiSpam for SMTP**, then click **Start**.

Uninstalling Symantec AntiSpam for SMTP

There are different instructions for uninstalling Symantec AntiSpam for SMTP on Solaris and Windows.

Uninstall Symantec AntiSpam for SMTP on Solaris

There may be files and registry entries that are not removed when you uninstall Symantec AntiSpam for SMTP. You must manually delete those files and entries.

Warning: If you are running other Symantec products, certain shared files, including registry files, should not be deleted.

If Symantec AntiSpam for SMTP was permitted to automatically disable conflicting services when it was installed, an attempt will be made during the uninstall process to reenable the services that were disabled during installation.

To uninstall Symantec AntiSpam for SMTP on Solaris

- Type the following command:
  pkgrm SYMCsass

To manually delete files and registry entries that are left behind after uninstalling

- Type the following commands:
  rm -r /var/opt/SASSMTP
  rm -r /opt/Symantec
  rm -f /etc/Symantec.com
  rm -f /etc/symantec.reg
  rm -f /var/log/SYMANTEC.error
  rm -f /var/log/SASSMTP-install.log
  These commands are based on default directory locations. If you changed the default directory locations, your commands will be different from those listed above.

Uninstall Symantec AntiSpam for SMTP on Windows NT/2000 Server

There may be files and registry entries that are not removed when you uninstall Symantec AntiSpam for SMTP. You must manually delete those files and entries.

To uninstall Symantec AntiSpam for SMTP on Windows

- Do one of the following:
  - In the Windows Control Panel, double-click **Add/Remove Programs**, click **Symantec AntiSpam for SMTP**, then click **Remove**.
  - On the Windows taskbar, click StartFrom the **Start** > **Programs** > **Symantec AntiSpam for SMTP** > **Uninstall Symantec AntiSpam for SMTP**.

To manually delete files that are left behind after uninstalling

1. Go to C:\Program Files\Symantec\SASSMTP.
2. Delete the **SASSMTP** folder.

Warning: If you are running other Symantec products, certain shared files, including registry files, should not be deleted.

To manually delete registry entries that are left behind after uninstalling

Warning: Do not delete registry events if you are running other Symantec products.

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run window, type **regedit**
3. Click **OK**.
4. In the Registry Editor window, under My Computer, double-click **HKEY_LOCAL_MACHINE**.
5. Double-click **SOFTWARE**.
6. Right-click the **Symantec** folder, then click **Delete**.
7. In the Confirm Key Delete window, click **Yes**.

Chapter 3

Configuring Symantec AntiSpam for SMTP

This chapter includes the following topics:

- Configuring administrator settings
- Configuring connection and delivery options
- Processing messages in the hold queue
- Configuring routing options
- Configuring alerts
- Configuring logging options
- Configuring diagnostic settings

Configuring administrator settings

There are two types of administrator accounts that can be set in Symantec AntiSpam for SMTP:

- Administrator: Oversees administration of Symantec AntiSpam for SMTP
- Report-only administrator: Has privileges only to run reports on Symantec AntiSpam for SMTP

Note: The report-only administrator password must be different from that of the administrator.

Configure administrator settings

Table 3-1 shows administrator settings that you can configure through the administrative interface.

Table 3-1 Administrator settings

Setting	Description
Administrator password	The administrator password is set during installation and can be changed through the administrative interface.
Report-only administrator password	The report-only administrator password can be set only through the administrative interface.
Administrator time-out	The administrator time-out applies to both the administrator and the report-only administrator accounts.
Administrator email addresses for notifications and alerts	The addresses to which notifications and alerts are sent when policy violations occur.

To change an administrator password through the administrative interface

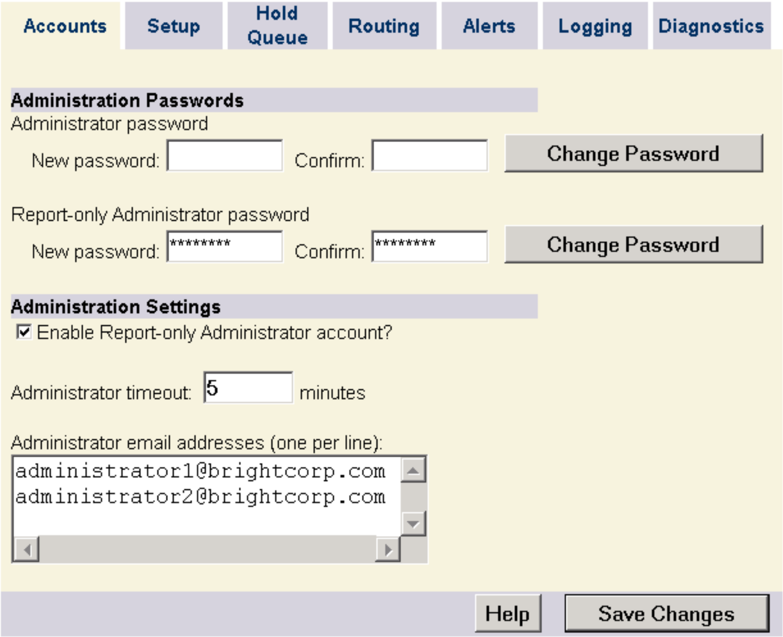
1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Passwords, under Administrator password, in the New password box, type a password for the administrator.

   Passwords are case sensitive.

   You do not need to set one through the interface unless you want to change the password you set during installation.
3. In the Confirm box, type the password again.
4. Click **Change Password**.

To set a report-only administrator password through the interface

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



Administration Passwords

Administrator password

New password: Confirm:

Report-only Administrator password

New password: ********* Confirm: *********

Administration Settings

☑ Enable Report-only Administrator account?

Administrator timeout: 5 minutes

Administrator email addresses (one per line):

```
administrator1@brightcorp.com
administrator2@brightcorp.com
```

2 On the Accounts tab, under Administration Passwords, under Report-only Administrator password, in the New password box, type a password for the report-only administrator.

Passwords are case sensitive.

3 In the Confirm box, type the password again.

4 Click **Change Password**.

To enable the report-only administrator account

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, check **Enable Report-only Administrator account**.
3. Click **Save Changes**.

Note: The report-only administrator password must be set before enabling the account.

To set the administrator time-out

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, in the Administrator timeout box, type the number of minutes that will elapse without activity before a new logon is required.
   Five minutes is the default.
   The administrator time-out applies to both the administrator and the report-only administrator.
3. Click **Save Changes**.

To set administrator email addresses for notifications and alerts

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Accounts tab, under Administration Settings, in the Administrator email addresses box, type the email addresses to which notifications and alerts will be sent.
   Type one email address per line.
3. Click **Save Changes**.
   In addition to setting an email address for notifications and alerts, you must configure Symantec AntiSpam for SMTP correctly to have it send notifications and alerts. This is done through the individual Notify and Alerts tabs.

Configuring connection and delivery options

You may configure the following in Symantec AntiSpam for SMTP:

- SMTP connection
  See "Configuring SMTP options" on page 27.
- Delivery options
  See "Configuring delivery options" on page 28.
- HTTP connection
  See "Configuring HTTP options" on page 29.
- HTTPS connection
  See "Configuring HTTPS options" on page 30.

Configuring SMTP options

Note: You may not use the same port number for SMTP, HTTP, or HTTPS. To change more than one port number to a port number that is used by another application, you must change one port number at a time. If you change more than one port number at a time, and you switch, for example, the port number that is used for HTTP with the port number that is used for HTTPS, you will receive an error message because Symantec AntiSpam for SMTP recognizes those port numbers as already being in use.

SMTP options apply to the Symantec AntiSpam for SMTP server, which receives email for processing and then forwards the email for delivery.

To configure SMTP options

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under SMTP, in the SMTP port number box, type the port number for the port on which Symantec AntiSpam for SMTP listens.
   The default is 25.
   If the SMTP port is reset to another port, only email that arrives at the other port will be processed. If a port number is entered that is already used, the SMTP port number reverts to the previously assigned port number and a warning message is displayed.

3 In the Maximum number of outgoing connections drop-down list, select the number of simultaneous connections for outgoing email.

The default is 30. Increasing the default increases resources required by the program and diminishes performance. Unless you have a compelling reason to do otherwise, accept the default.

Additional connections are queued when the system is already processing the maximum number of connections that are allowed.

Multiprocessor computers can effectively use more connections than single processors.

4 On the Maximum number of incoming connections menu, select the number of simultaneous connections for incoming email.

The default is 15. Unless you have a compelling reason to do otherwise, accept the default.

Setting the number of connections too high can slow processing. Additional connections are queued when the system is already processing the maximum number allowed.

5 In the Alert/Notification “From:” box, type the text that you want to appear in the From field when Symantec AntiSpam for SMTP notifications are sent.

The default is Symantec_AntiSpam _for_SMTP.

Warning: Do not type an actual administrative email account name in the From field. Software logic prevents message looping due to bounces by dropping all email destined to this From account. This means that if you enter an email account name in the From field, all email destined for that account will be dropped.

6 Click **Save Changes**.

Configuring delivery options

During a virus outbreak, you may want to pause delivery of messages or reject incoming messages.

You can also specify the number of days to attempt to deliver a message.

Configure delivery options

Follow these instructions to pause delivery, reject incoming messages, and set the number of days to attempt message delivery.

To pause delivery of messages

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Setup tab, under Delivery, check **Pause message delivery**.
While this is checked, messages are still received and placed in the fast queue, but no messages are delivered. Once it is unchecked, the stored messages are delivered as usual.

3 Click **Save Changes**.

To reject incoming messages

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Setup tab, under Delivery, check **Reject incoming messages**.
While this is checked, no incoming messages are accepted, and the sending server receives notification that the service is not available. Once it is unchecked, incoming messages are processed as usual.

3 Click **Save Changes**.

To set the number of days to attempt message delivery

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Setup tab, under Delivery, in the Number of days list, select the number of days that Symantec AntiSpam for SMTP will attempt to deliver a message.
Once a message cannot be delivered, it is sent to the slow queue where Symantec AntiSpam for SMTP continues to attempt delivery. If a message cannot be delivered after the set number of days, it is returned to the sender and deleted from the slow queue and from the system.

3 Click **Save Changes**.

Configuring HTTP options

The Symantec AntiSpam for SMTP software is managed through a Web-based interface. This interface is provided through a built-in Hypertext Transfer Protocol (HTTP) server that is included with the software. This HTTP server is independent of any existing HTTP server that is already installed on your server and is not a general-purpose Web server.

The HTTP port number is set during installation, but it can be changed through the administrative interface.

To configure HTTP options

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, under HTTP/HTTPS, in the HTTP port number box, type the port number on which the built-in HTTP server will listen.

   The number that you specify becomes the port number in the URLs that you will use to access the Symantec AntiSpam for SMTP administrative interface. The port number must be exclusive to Symantec AntiSpam for SMTP and must not already be in use by any other program or service.

   Because the built-in HTTP server is not a general purpose Web server, do not use port number 80 (the default port number for general-purpose Web servers). Unless you have a compelling reason to do otherwise, you should use the default port number of 8003. If you select a port number other than the default, do not forget which port number you selected.
3. Click **Save Changes**.

Configuring HTTPS options

During installation, you must identify the port number for your HTTPS server. You can define an HTTPS server connection between computers on your network and Symantec AntiSpam for SMTP for SSL encryption of passwords during logon sessions.

Note: You must have an SSL Web server certificate installed prior to enabling SSL encryption for logons.

Configure HTTPS options

You must do the following to configure HTTPS options:

- Generate an SSL certificate request.
- Submit the certificate request to a recognized Certificate Authority.
- Install the certificate that is returned from the Certificate Authority.
- Enable SSL encryption.

To generate an SSL certificate request

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Setup tab, in the HTTPS port number box, type the port number of the HTTPS server.

   The default port number is 8043. The port number must be exclusive to Symantec AntiSpam for SMTP and must not already be in use by any other program or service.
3. Click **Certificate Management**.
4. In the Certificate Management window, under Request, in the Common Name box, type the IP address or resolvable host name of the computer that is running Symantec AntiSpam for SMTP (for example, smart.brightschool.com).

   Check the Web site of the Certificate Authority to which the request will be submitted to see if there are format restrictions. For example, some Certificate Authorities require a resolvable host name instead of an IP address. Some require that the state or province name be spelled out.
5. In the Organization box, type the name of your organization (for example, Bright School).
6. In the Organization Unit box, type your business's main function (for example, Education).
7. In the City/Locality box, type your city or locality.
8. In the State/Province box, type your state or province.

   If you do not have a state or province, you must type something in this field.
9. In the Country/Region list, select your country or region.
10. In the E-mail Address box, type your email address.

    The certificate will be sent to the email address that is entered in this box.
11. Click **Create Request**.

    The certificate request is displayed in the Certificate Management Request window.

To submit the certificate request to a recognized Certificate Authority

1. In the Certificate Management Request window, copy the entire request, including the header and footer, to your clipboard or to a text file.
2. Click **OK**.

3 Submit the clipboard contents or the copied text file to a recognized Certificate Authority (for example, VeriSign®) by pasting it on the Certificate Authority's site, as they direct.
The Certificate Authority emails your certificate to the address that you typed on the Certificate Request page.

To install the returned certificate on the Symantec AntiSpam for SMTP server

1 Copy the entire certificate, including the header and footer, received via email from the Certificate Authority.

2 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

3 On the Setup tab, under HTTP/HTTPS, click **Certificate Management**.

4 In the Certificate Management window, under Install, paste the copied certificate, including the header and the footer.

5 Click **Install Certificate**.

To enable SSL encryption

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Setup tab, under HTTP/HTTPS, check **Enable SSL & encryption for logons**.

3 Click **Save Changes**.
In the Certificate Management window, under Status, you should now see the following:

- Date on which the private key was installed
This was done automatically when you generated your request.
- Date on which the certificate was installed
- Date on which the certificate expires
Expiration information is displayed only when SSL is enabled.

Acting as your own Certificate Authority

If you are able to act as your own Certificate Authority, you need only install a valid certificate on the Symantec AntiSpam for SMTP server and enable SSL encryption for logons.

See "To install the returned certificate on the Symantec AntiSpam for SMTP server" on page 32 and "To enable SSL encryption" on page 32.

Processing messages in the hold queue

If a message causes a system crash three times, it is moved to the hold queue.

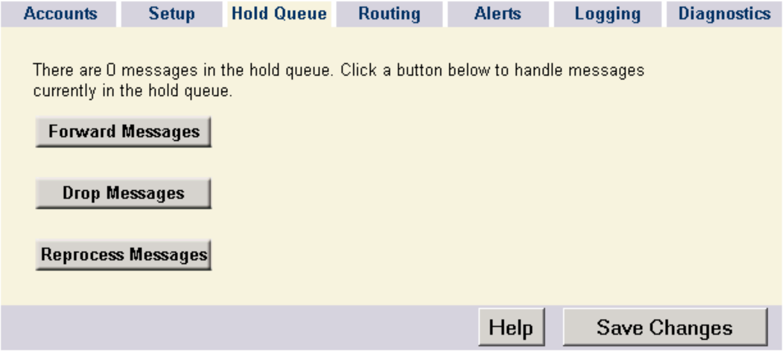
Process messages in the hold queue

You can configure Symantec AntiSpam for SMTP to reprocess, drop, or forward a copy of messages in the hold queue.

Warning: Reprocessing messages is not recommended. Reprocessing a message that has caused a system crash will likely result in another system crash.

To reprocess messages that are in the hold queue

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



There are 0 messages in the hold queue. Click a button below to handle messages currently in the hold queue.

2 On the Hold Queue tab, click **Reprocess Messages**.

3 In the Reprocessing Hold Queue Messages window, click **Yes**.
All messages that are in the hold queue are reprocessed.

To drop messages that are in the hold queue

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Hold Queue tab, click **Drop Messages**.

3 In the Dropping Hold Queue Messages window, click **Yes**.
All messages that are in the hold queue are dropped from your system and are not delivered.

To forward messages that are in the hold queue

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Hold Queue tab, click **Forward Messages**.
3. In the Forwarding Hold Queue Messages window, click **Yes**.
4. In the Subject box, type the subject for the forwarded email messages.
5. In the Email address box, type one email address to which email messages in the hold queue are to be forwarded.
6. Click **Forward**.
   Copies of messages in the hold queue are forwarded. Copies are not scanned. Originals remain in the hold queue until they are dropped or manually deleted.

Configuring routing options

Symantec AntiSpam for SMTP processes email messages and then routes them to your existing hosts for delivery. There are two routing configurations:

- Default routing
  See “Configuring default routing” on page 34.
- Local routing
  See “Configuring local routing” on page 36.

Configuring default routing

Setting default routing is not required in most environments but must be done if no local routing is set.

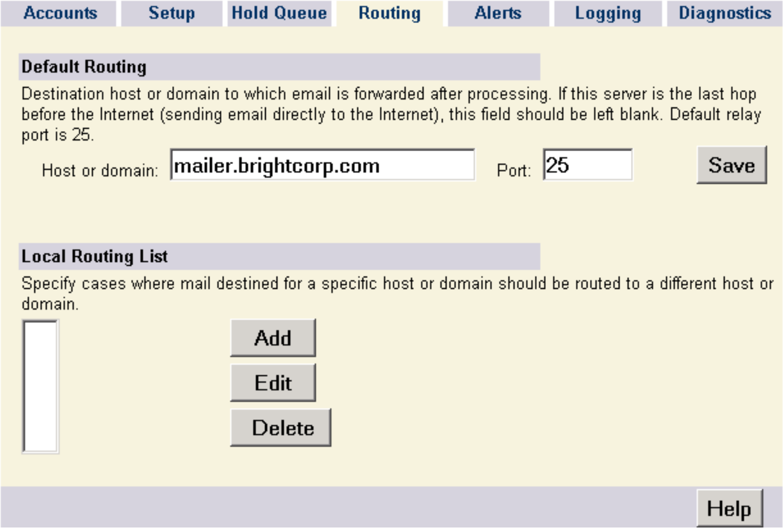
See “Preventing spam relaying” on page 55.

If the Default Routing box is filled in, any email that is not addressed to a host or domain in the local routing list (a name by itself or the name on the left side of an arrow) will be forwarded to the server on your network that is listed in the Default Routing box.

If this box is not filled in, any email that is not addressed to a name in the local routing list will be delivered to the appropriate SMTP server on the Internet.

To configure default routing

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



Default Routing

Destination host or domain to which email is forwarded after processing. If this server is the last hop before the Internet (sending email directly to the Internet), this field should be left blank. Default relay port is 25.

Host or domain: mailer.brightcorp.com Port: 25

Local Routing List

Specify cases where mail destined for a specific host or domain should be routed to a different host or domain.

2 On the Routing tab, under Default Routing, in the Host or domain box, type the fully qualified host name or IP address of your mail server.

3 In the Port box, type the port number of your mail server.
The default port number is 25.

4 Click **Save**.

Mail that was destined for your SMTP server goes to Symantec AntiSpam for SMTP for processing and then is forwarded to the specified SMTP server for delivery.

Configuring local routing

Note: You must set a routing list entry for each email domain on your network with the domain (for example, brightcorp.com) as the routed host or domain and your mail server as the destination relay.

Setting local routing is required in most environments and is essential if you are not using default routing. The typical setting for most environments is an email domain routed to an SMTP server.

The local routing list has two purposes:

- It defines special rules for relaying processed email.
- It identifies which domains and hosts are considered local.

There are two types of local routing entries:

- A name by itself
  A name by itself means that Symantec AntiSpam for SMTP treats email addressed to that host name, domain, or IP address as local and does a DNS lookup for the address and delivers it where the MX record directs it.
- A name followed by another name
  A name followed by another name means that when Symantec AntiSpam for SMTP receives and processes email addressed to the host name, IP address, or domain of the first mail server that it should use the second name to relay the mail.
  For example, if you type brightcorp.com in the Routed host or domain box and mailer.brightcorp.com in the Destination relay box, after Symantec AntiSpam for SMTP processes email addressed to brightcorp.com (user@brightcorp.com), it forwards the email to mailer.brightcorp.com for delivery.

In both cases, the first (or only) name is considered local. The second name (if any) is not. Local routing rules always have priority over the Default Routing setting.

Designating a host as local is significant for the relay restrictions.

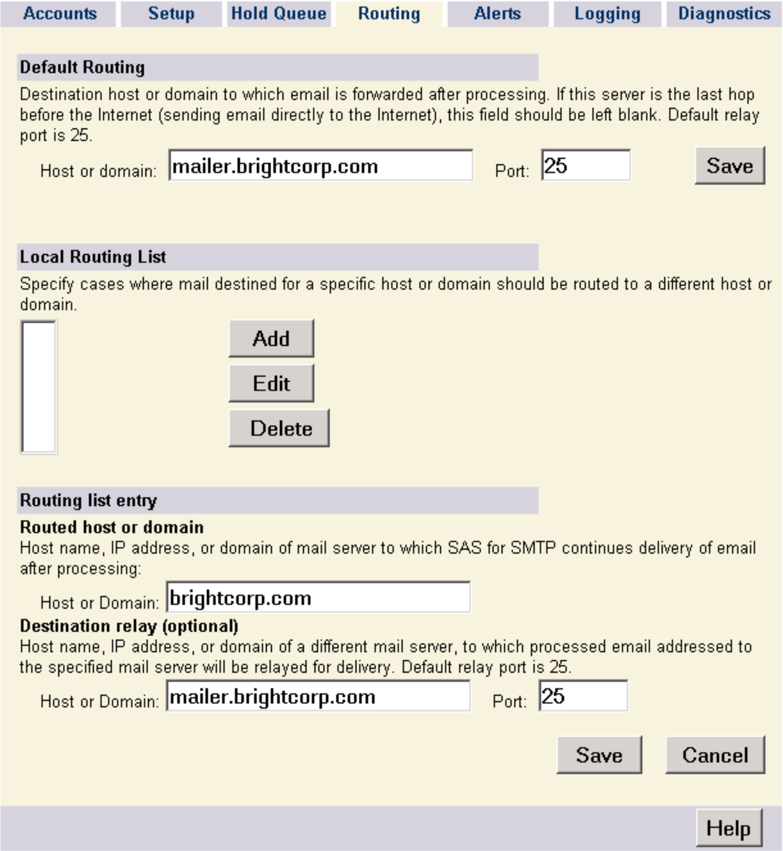
See “Preventing spam relaying” on page 55.

Configure local routing

You can create, edit, and delete local routing list entries.

To create local routing entries

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



Default Routing

Destination host or domain to which email is forwarded after processing. If this server is the last hop before the Internet (sending email directly to the Internet), this field should be left blank. Default relay port is 25.

Host or domain: mailer.brightcorp.com Port: 25

Local Routing List

Specify cases where mail destined for a specific host or domain should be routed to a different host or domain.

Routing list entry

Routed host or domain

Host name, IP address, or domain of mail server to which SAS for SMTP continues delivery of email after processing:

Host or Domain: brightcorp.com

Destination relay (optional)

Host name, IP address, or domain of a different mail server, to which processed email addressed to the specified mail server will be relayed for delivery. Default relay port is 25.

Host or Domain: mailer.brightcorp.com Port: 25

2. On the Routing tab, under Local Routing List, click **Add**.

3. Under Routing list entry, type the host name, IP address, or domain of a mail server to which email should be routed.

   Wildcard characters may be used in routing list entries.

   If you type only the first entry and no destination relay, email that is addressed to a user who receives mail at that host will be relayed using that host.

4 Under Destination relay, in the Host box, type the host name, IP address, or domain of the mail server to which email that is destined for the server that is designated above should be routed.

If you type a destination host, email addressed to a user receiving mail at the host listed under Routed host or domain will be relayed using the host typed in the Host box under Destination relay.

5 In the Port box, type the port number for the mail server.

The default port number is 25.

6 Click **Save**.

To edit a local routing list entry

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the entry that you want to edit.

3 Click **Edit**.

4 Make the changes that you want.

5 Click **Save**.

To delete a local routing list entry

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Routing tab, under Local Routing List, select the entry that you want to delete.

3 Click **Delete**.

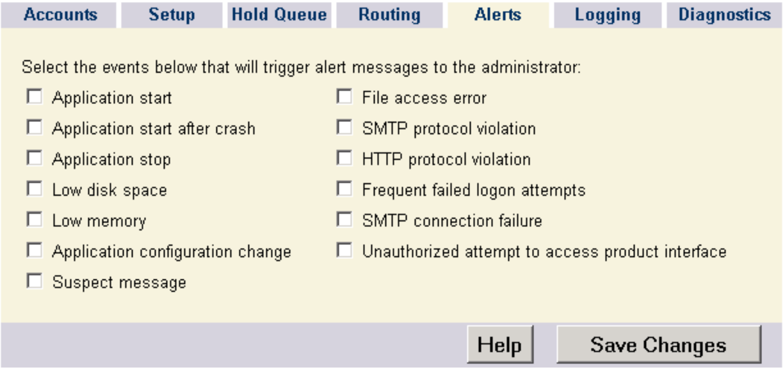
Configuring alerts

You can configure Symantec AntiSpam for SMTP to send alerts to one or more administrators for system events.

Note: If no email address is specified, alerts will not be delivered.
See "To set administrator email addresses for notifications and alerts" on page 26.

To configure alerts

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



Select the events below that will trigger alert messages to the administrator:

☐ Application start
☐ Application start after crash
☐ Application stop
☐ Low disk space
☐ Low memory
☐ Application configuration change
☐ Suspect message
☐ File access error
☐ SMTP protocol violation
☐ HTTP protocol violation
☐ Frequent failed logon attempts
☐ SMTP connection failure
☐ Unauthorized attempt to access product interface

2 On the Alerts tab, select the events that will trigger alerts to the administrator.
The alerts will be sent to the email addresses that you designated when configuring administrative settings.

3 Click **Save Changes**.

Table 3-2 shows system events that trigger alerts, their descriptions, and examples of alerts.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
Application start	The application has started.	Subject: Application Start Body: The application has been started.
Application start after crash	The server has started after an unexpected shutdown.	Subject: Application Start after Crash Body: The server has been started after an unexpected shutdown.
Application stop	The server has stopped.	Subject: Application Stop Body: The application has been stopped.
Low disk space	The disk space in the logging, email scanning, or mail queuing directory is less than 10 percent.	Subject: Low Disk Space Threshold Exceeded Body: The [ ] directory is running dangerously low on disk space, where [ ] is either logging, email, or mail queuing.
Low memory	Less than 10 percent of memory remains.	Subject: Low Memory Threshold Exceeded Body: The memory available on the server is running dangerously low.
Application configuration change	The software has been reconfigured in some way.	Subject: Configuration Change Body: A configuration change was made.
Suspect message	On the third attempt to send a message that crashes Symantec AntiSpam for SMTP, the message is considered suspect and moved to the hold queue.	Subject: Suspect Message Body: A suspect message was received by the server.
File access error	A user has attempted to access a file for which the user has no permissions, or a file has been altered and, therefore, cannot be accessed.	Subject: File Access Error Body: A file access error occurred on the server.

Table 3-2 Events that trigger alerts

Event	Description	Alert text
SMTP protocol violation	During authentication, a protocol violation between SMTP servers has been detected.	Subject: SMTP Protocol Violation Body: An SMTP protocol violation was detected by the server.
HTTP protocol violation	During authentication, a protocol violation with the HTTP server has been detected.	Subject: HTTP Protocol Violation Body: An HTTP protocol violation was detected by the server.
Frequent failed logon attempts	Three unsuccessful logon attempts have been made. An alert is sent on the third attempt, and one is sent for every unsuccessful attempt thereafter. The counter is reset upon correct logon.	Subject: Frequent Failed Logon Attempts Body: Several failed logon attempts have been made to the server.
SMTP connection failure	The SMTP server that Symantec AntiSpam for SMTP is trying to contact is not available.	Subject: SMTP Connection Failure Body: A connection failure was encountered by the server.
Unauthorized attempt to access product interface	Users, including report-only administrators, have attempted to access the administrative interface without appropriate permissions.	Subject: Unauthorized Attempt to Access Product Interface Body: An unauthorized attempt to access the server interface was detected.

Configuring logging options

There are two types of logging available in Symantec AntiSpam for SMTP: local logging and SESA logging. Local logging (logging of activity to the computer on which Symantec AntiSpam for SMTP is running) is enabled by default. For local logging, you can specify how long old logs should be retained, from one week to never delete.

SESA logging (logging of activity to the SESA Console) is not enabled by default.

See “To configure logging options” on page 43 and “Integrating Symantec AntiSpam for SMTP with SESA” on page 69.

Once enabled, Symantec AntiSpam for SMTP logs the following local events to SESA:

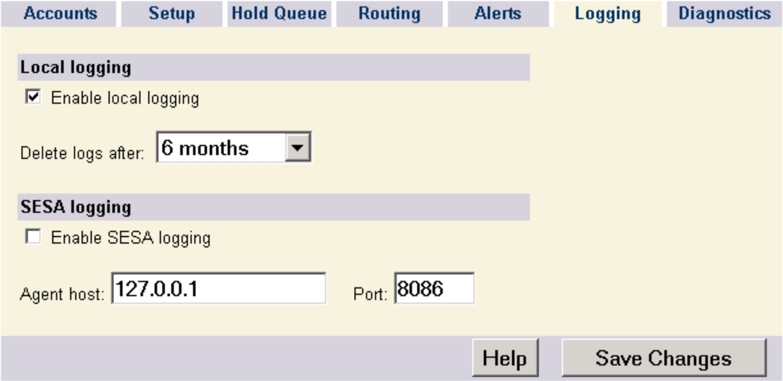
- Logon
- Logoff
- Object modified
- Service started
- Service stopped
- Reordering started
- Reordering stopped
- Connection from
- Connected to
- Disconnected
- Connection closed
- Protocol violation
- Rejected
- Accepted
- Dropped
- Bounced
- Delivered
- Delivery failed
- Delivery suppressed
- Held
- Completed
- Subjects blocked
- Sender blocked
- Spam list block
- Spam detection

See “Generating detail reports” on page 65.

Since no data is being retained while logging is disabled, it is impossible to generate reports during any period during which logging is disabled.

To configure logging options

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.



Local logging

☑ Enable local logging

Delete logs after: 6 months

SESA logging

□ Enable SESA logging

Agent host: 127.0.0.1 Port: 8086

2 On the Logging tab, under Local logging, check or uncheck Enable local logging.

3 In the Delete logs after list, select the time period to retain log files.

4 Under SESA logging, check or uncheck Enable SESA logging.

5 In the Agent host box, type the IP address on which the Agent listens.

6 In the Port box, type the port number on which the Agent listens.

7 Click **Save Changes**.

Configuring diagnostic settings

Diagnostic files are located on Windows in the queues folder and on Solaris in the DiagDir directory. If you contact Symantec Technical Support for assistance, you may be instructed to configure the diagnostic settings.

Warning: The default for the diagnostic settings is Disable. Do not change these settings unless you are instructed by Symantec Technical Support to do so. Changing the settings affects throughput and resource utilization.

Configuring queue file save

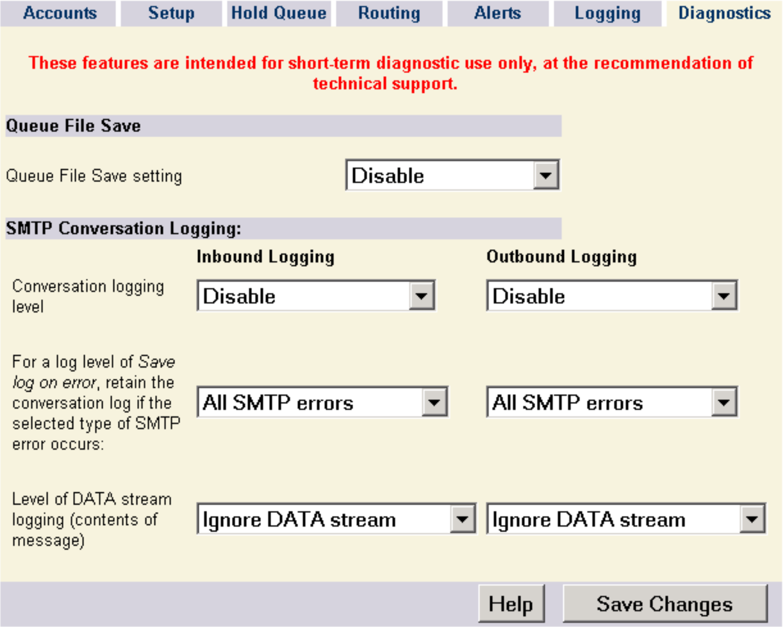
There are options for configuring queue file save.

To configure queue file save

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Diagnostics tab, under Queue File Save, in the Queue File Save setting list, select the setting that Symantec Technical Support tells you to select.

3 Click **Save Changes**.



These features are intended for short-term diagnostic use only, at the recommendation of technical support.

Queue File Save

Queue File Save setting: Disable

SMTP Conversation Logging:

	Inbound Logging	Outbound Logging
Conversation logging level	Disable	Disable
For a log level of *Save log on error*, retain the conversation log if the selected type of SMTP error occurs:	All SMTP errors	All SMTP errors
Level of DATA stream logging (contents of message)	Ignore DATA stream	Ignore DATA stream

Configuring SMTP conversation logging

You can now configure SMTP protocol conversation logging, which logs the incoming or outgoing SMTP protocol conversation when accepting or delivering a message. If inbound logging is enabled, one conversation log is generated for each inbound connection. If outbound logging is enabled, one log is generated for each message delivery attempt.

Note: Conversation log files are saved to the diagnostic files directory defined during installation (default location is <InstallDir>/queues/diagnosticfiles, where <InstallDir> is the path of the top-level installation directory, such as var/opt/SASSMTP or C:\Program Files\Symantec\SASSMTP.

To configure conversation logging

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.
2. On the Diagnostics tab, under SMTP Conversation Logging, in the logging lists, choose one of the following for the conversation logging level:
   - Disable: No conversation logging is performed.
   - Save log on error: Conversation logs are saved only if an SMTP error occurs during the message transmission.
   - Log all inbound (or outbound) traffic: All conversation logs are saved for inbound or outbound conversations.
3. On the Diagnostics tab, under SMTP Conversation Logging, in the logging lists, choose one of the following to determine error type triggers:
   - All SMTP errors: All SMTP errors are logged.
   - Communication error: Network and socket errors are logged.
   - Protocol error: Failures to follow defined SMTP protocols (such as a command out of sequence or bad syntax) are logged.
   - Local processing error: Application-defined errors (such as a message that exceeds defined size limits) are logged.
   - Unsupported operation: Requests for unsupported operations (such as TURN) are logged.

4. On the Diagnostics tab, under SMTP Conversation Logging, in the logging lists, choose one of the following to determine the level of DATA stream logging:
    - Ignore DATA stream: Only the DATA command is logged.
    - Summarize DATA stream: A line count and byte count summary of the DATA stream is logged.
    - Echo DATA stream: The entire DATA stream is logged.

Note: For outbound messages, the DATA stream is buffered. The line count and byte count of the DATA stream for outbound messages will not match the line count and byte count for inbound messages.

Chapter 4

Setting your blocking policy

This chapter includes the following topics:

- About your blocking policy
- Blocking by message criteria
- Blocking spam
- Preventing spam relaying

About your blocking policy

Your blocking policy is determined by how you configure Symantec AntiSpam for SMTP to block messages (for example, what criteria to use to block messages and how those blocked messages and attachments are to be handled).

Table 4-1 shows the criteria that you can use to block messages and how those blocked messages can be handled.

Table 4-1 Blocking criteria

Criteria	Handling options
Message size	Email messages that exceed the size that is specified in megabytes are not accepted at the SMTP server. Not blocking messages based on size is the default.
Subject line	Email messages with specified subject lines may be dropped, logged, or forwarded. Not identifying subject lines is the default.

Table 4-1 Blocking criteria

Criteria	Handling options
Sender's address	Email messages that are from specified email addresses or domains are blocked. Not blocking messages based on sender's address is the default.
DNSBL antispam list	Email messages that are from domains listed in the Domain Name Server Black List (DNSBL) services that you specify are blocked.
Anti-relay settings	Email messages with non-local destinations are handled according to how you configure Symantec AntiSpam for SMTP. Do not allow, except for listed hosts is the default.
Characters in addresses	Email messages with characters specified to be blocked are not accepted by the SMTP server. Not blocking by characters in email addresses is the default.

Blocking by message criteria

Symantec AntiSpam for SMTP can be configured to block messages based on the following content:

- Message size
  See "Blocking by message size" on page 48.
- Subject line
  See "Blocking by subject line" on page 49.

Blocking by message size

You can configure Symantec AntiSpam for SMTP to block email by message size.

To block by message size

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.
2. In the Content window, on the Configure tab, under Blocking by message size, check **Reject messages that are greater than [ ] megabytes**.
   The default is 50.
3. In the text box, type the number of megabytes that must be exceeded for a message to be rejected.
   Do not use a decimal.
4. Click **Save Changes**.

Blocking by subject line

You can configure Symantec AntiSpam to block email by subject line.

To block by subject line

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.
2. In the Content window, on the Configure tab, under Blocking by subject line, check **Identify the following subject lines (one per line) as content violations**.
3. In the subject line box, type the subject lines, one per line, that Symantec AntiSpam for SMTP will block.
   Subject line blocking is not case sensitive.
   You can use the * and ? wildcards, for example, *hot* would block any subject line that contains the character string hot.
4. Under Take the following action when a subject line violation occurs, select one of the following:
   - Drop message
   - Log only
   - Forward message
5. If you selected Forward message, in the To email address box, type one address to which the rejected message will be forwarded, and in the Subject line box, type the subject line of the rejected message to be forwarded.
6. Click **Save Changes**.

Blocking spam

Symantec AntiSpam for SMTP can block spam in the following ways:

- Block by a sender's email address.
- Block by Domain Name Server Black List (DNSBL) anti-spam lists.
  You can create an anti-spam white list so that email from the domains contained in the white list are excluded from spam processing.
- Identify suspected spam messages by the heuristic spam engine.

Blocking by a sender’s email address

You can configure Symantec AntiSpam for SMTP to block email by a sender’s address or domain. It searches both the “envelope From” and “message From:” headers to determine string matches.

Domain names must begin with either @ or a period.

Note: If you configure Symantec AntiSpam for SMTP to block a subdomain (server.company.com, for example), it blocks only that subdomain and not the full domain (company.com, for example).

To block by a sender’s address

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.

2 In the Antispam window, on the Configure tab, under Blocking by sender’s address, check **Identify messages from the following email addresses or domains as violations (one per line)**.

3 In the text box, type the email addresses and domains to be blocked.
There must be only one entry per line.

4 Under Do the following when a violation occurs, select one of the following:

- Drop message
- Log only
- Forward message

5 If you selected Forward message, in the To email address box, type the email address to which the message will be forwarded, and in the Subject box, type the subject that will appear in the subject line of the forwarded message.

6 Click **Save Changes**.

Blocking by DNSBL anti-spam lists

The most common way of preventing spam is rejecting mail that comes from mail servers known or believed to send spam. To limit potential spam, Symantec AntiSpam for SMTP can support up to three DNS black lists (DNSBL). DNSBL is a DNS-based blocking list generated to limit spam. You may choose to use these lists to reject or tag mail from certain sources, based on criteria determined by the list operators, such as return codes associated with Internet mail servers known to act as open relays or dial-up IPs used by spammers. DNSBL depends on an actively maintained DNS server with a database of IP addresses associated with Internet mail servers judged to be abusive on one or more spam-related criteria.

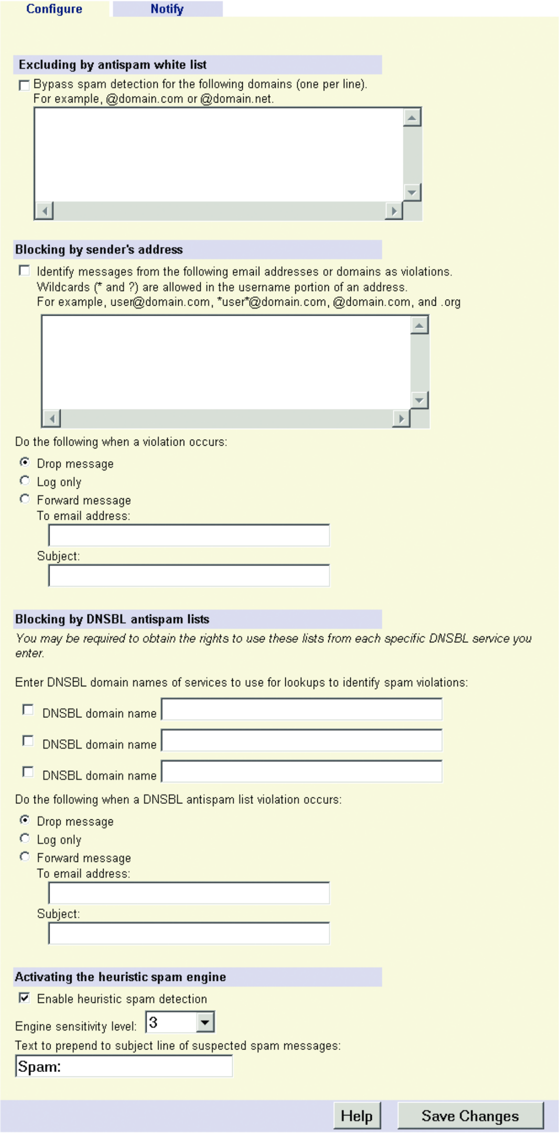
Symantec AntiSpam for SMTP uses the IP session of the open connection request from a sending mail host to query the DNSBL. If the query response indicates that the return code is listed in the DNSBL database, then Symantec AntiSpam for SMTP refuses the connection attempt.

In Symantec AntiSpam for SMTP, administrators can specify up to three domains to query against.

Note: If the check box for the DNSBL service is not checked, Symantec AntiSpam for SMTP does not attempt to use the service, even if a domain name is entered for a spam service.

To block by DNSBL anti-spam lists

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.



Excluding by antispam white list

□ Bypass spam detection for the following domains (one per line).
For example, @domain.com or @domain.net.

Blocking by sender's address

□ Identify messages from the following email addresses or domains as violations.
Wildcards (* and ?) are allowed in the username portion of an address.
For example, user@domain.com, *user*@domain.com, @domain.com, and .org

Do the following when a violation occurs:

● Drop message
○ Log only
○ Forward message
To email address:
Subject:

Blocking by DNSBL antispam lists

You may be required to obtain the rights to use these lists from each specific DNSBL service you enter.

Enter DNSBL domain names of services to use for lookups to identify spam violations:

□ DNSBL domain name
□ DNSBL domain name
□ DNSBL domain name

Do the following when a DNSBL antispam list violation occurs:

● Drop message
○ Log only
○ Forward message
To email address:
Subject:

Activating the heuristic spam engine

☑ Enable heuristic spam detection

Engine sensitivity level: 3

Text to prepend to subject line of suspected spam messages:
Spam:

2 In the Antispam window, on the Configure tab, under Blocking by DNSBL antispam lists, check **DNSBL domain name**.

3 In the DNSBL domain name box, type the domain of the DNS service that you request.

A check box will appear to let you identify spam by return codes. If desired, select the box, and a box will appear to let you type return codes to identify email as spam.

4 Type one return code per line (from the selected services) to identify email as spam.

Identifying return codes means that only the email associated with the entered return codes will be blocked.

To handle anti-spam list violations

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.

2 In the Antispam window, on the Configure tab, under Blocking by DNSBL antispam lists, under Do the following when a DNSBL antispam list violation occurs, select one of the following:

- Drop message
- Log only
- Forward message

3 If you selected Forward message, in the To email address box, type one address to which the message will be forwarded, and in the Subject line box, type the subject line to appear for the subject of the forwarded message.

4 Click **Save Changes**.

Excluding by anti-spam white lists

You can choose to specify domains so that email from those domains is excluded from spam processing. If both DNSBL and exclusion are activated, Symantec AntiSpam for SMTP checks the anti-spam white list first when spam processing begins, after which the DNSBL black lists are queried. If the envelope sender matches a domain entered in the anti-spam white list, the email is allowed. If it does not match, DNSBL lists are checked. If there is a match, the email is blocked.

Email from domains listed in the white list are still processed for content violations.

To exclude by anti-spam white lists

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.

2 In the Antispam window, on the Configure tab, under Excluding by anti-spam white list, check **Bypass spam detection for the following domains (one per line)**.

3 In the exclusion box, type the domains (one per line) to be excluded from regular spam processing.
Domain names must begin with either @ or a period.

Note: You must have Bypass spam detection for the following domains (one per line) checked in order for the domains entered to bypass spam processing.

Identify suspected spam messages by the heuristic spam engine

The heuristic spam engine is active by default. It performs an analysis on the entire incoming email message, looking for key characteristics of spam. It weighs its findings against key characteristics of legitimate email, and assigns an accuracy rating (for example, 98 percent) to how certain it is that the message is spam. This rating, in conjunction with the engine sensitivity level (1=low, 5=high), determines whether a message is considered spam.

Note: Three (3) is the default sensitivity level for the heuristic anti-spam engine. Increasing the sensitivity level may result in more false positives.

To identify suspected spam messages by the heuristic spam engine

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.

2 In the Antispam window, on the Configure tab, under Activating the heuristic spam engine, do the following:

- Check **Enable heuristic spam detection**.
- Select the engine sensitivity level.
- Type the text that will be prepended to the subject line of suspected spam messages.

3 Click **Save Changes**.

Preventing spam relaying

Spam is unsolicited commercial email. You can configure relay restrictions within Symantec AntiSpam for SMTP so that it refuses to deliver email that has both a source and a destination outside of the organization (email for which neither the sender nor the receiver is local).

Another way that Symantec AntiSpam for SMTP prevents spam relaying is by rejecting messages with addresses that contain characters that are commonly associated with spam relaying, such as ! and %.

Configuring external relay restrictions

Two relay options are available:

- Allow: Relay restrictions are disabled for external hosts. Email from any remote host can be relayed through Symantec AntiSpam for SMTP to remote hosts.
- Do not allow, except for listed hosts (one per line): Relay restrictions are enabled for external hosts. Only email from explicitly named hosts and domains can be relayed to remote hosts.
  Do not allow, except for listed hosts (one per line) is the default.

The source of a message is the computer that contacts Symantec AntiSpam for SMTP, not the From address. The destination is the host portion of the recipient's address. If the source or destination is considered local, the Do not allow setting does not apply.

See "To configure external relay restrictions" on page 56.

If a message has multiple recipients, each recipient is considered individually for relay restrictions.

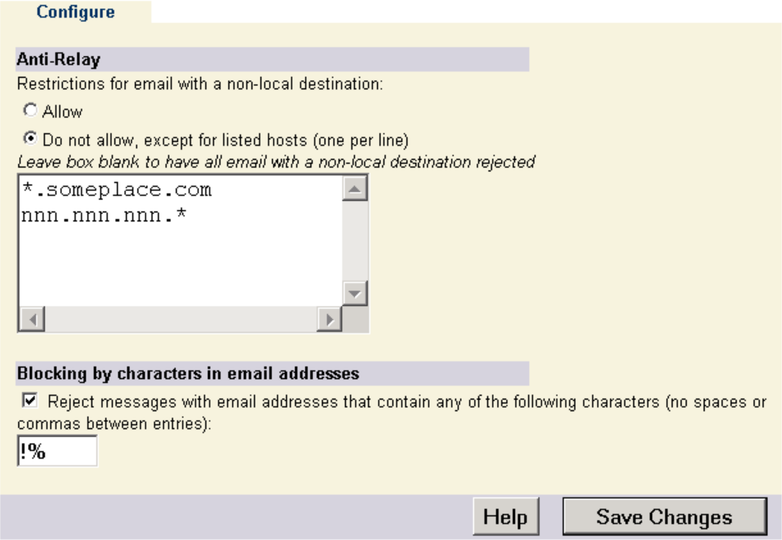
A source is considered local if Symantec AntiSpam for SMTP is running in Allow mode, or if the host is listed in the Do not allow, except for listed hosts list.

A destination is considered local if it is listed in the Local Routing list.

See "Configuring local routing" on page 36.

To configure external relay restrictions

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.



Anti-Relay

Restrictions for email with a non-local destination:

○ Allow

● Do not allow, except for listed hosts (one per line)

Leave box blank to have all email with a non-local destination rejected

```
*.someplace.com
nnn.nnn.nnn.*
```

Blocking by characters in email addresses

☑ Reject messages with email addresses that contain any of the following characters (no spaces or commas between entries):

!%

2 In the Anti-Relay window, on the Configure tab, select one of the following:

- Allow
- Do not allow, except for listed hosts (one per line)

3 If desired, type one host name, IP address, or domain per line for mail servers from which email will be allowed.

Domain name entries in this box will work only if the hosts have appropriate PTR records to map IP addresses to domain names.

You can use the * wildcard to specify allowed hosts as the first element of a domain name or the last element of an IP address. For example:

*.someplace.com

1.2.3.*

1.2.*

1.*

If Do not allow is selected, and no hosts are listed, Symantec AntiSpam for SMTP rejects all email with a non-local destination.

4 Click **Save Changes**.

Blocking by characters in email addresses

You can configure Symantec AntiSpam for SMTP to reject messages with email addresses that contain characters that are commonly associated with spam relaying, such as ! and %.

To block by characters in email addresses

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Blocking Policy**.
2. In the Anti-Relay window, on the Configure tab, under Blocking by characters in email addresses, check **Reject messages with email addresses that contain any of the following characters**.
3. In the text box, type one or more characters for which Symantec AntiSpam for SMTP will search for email addresses to block.
   Do not insert spaces or commas between the entries.
4. Click **Save Changes**.

Chapter 5

Notifications, logging, and reporting

This chapter includes the following topics:

- About the Status page
- About notifications
- Generating reports

About the Status page

When you log on to Symantec AntiSpam for SMTP, the Status page is displayed. This page shows system metrics that were calculated from the time of the most recent startup.

At the bottom of the window, you can click Refresh to update the display to reflect current, real-time status.

Note: Symantec AntiSpam for SMTP attempts a separate delivery for each recipient, and the results are tracked individually. On the Status page, the number of Messages Delivered is often greater than the number of Messages Accepted because of multiple recipients.

Table 5-1 shows the information that appears on the Status page.

Table 5-1 Status page information

Topic	Information
Status	■ Server and port number for Symantec AntiSpam for SMTP ■ Version number of the product: 3.1 ■ Date on which the server was last started ■ Amount of time that the server has been running since it was last started ■ Total number of megabytes that have been received for processing since the server was last started ■ Message delivery status: Delivery or Pause ■ Incoming message status: Accept or Reject ■ Date on which the SSL certificate was installed, or Not installed
Messages	■ Accepted: Number of messages added to the fast queue since the server was last started ■ Rejected: Number of messages rejected because the software is configured to reject messages, disallowed characters are in an email address, an anti-relay violation occurs, or the configured message size has been exceeded ■ Delivered: Number of outgoing messages that have been delivered ■ Dropped: Number of messages dropped because the software is configured to drop messages in any of the following cases: attachments are not repaired or deleted, subject lines are disallowed, container limit has been exceeded, encrypted container has been detected, disallowed sender's address has been detected, block by anti-spam list, scan error, scan failure ■ Held: Number of messages that have been added to the hold queue since the last restart, including those dropped by the administrator ■ Forwarded: Number of messages that have been forwarded successfully to the administrator addresses See "To set administrator email addresses for notifications and alerts" on page 26.
Queue status	■ Number of messages currently in fast queue ■ Number of messages currently in slow queue ■ Number of messages currently in hold queue

About notifications

You can configure Symantec AntiSpam for SMTP to send notifications to senders and administrators when the blocking policy has been violated.

Understanding sender notifications

Table 5-2 shows sender notification information.

Table 5-2 Sender notification information

Event	Default subject	Default message	Other information
Content violation	Content violation	Content violation found in email message.	■ From/To information ■ Content violation that occurred (blocked because of message size or subject line)
Spam **Note:** Notification is not sent when spam is detected by the heuristic spam engine.	Email not allowed	A message sent by this account comes from a domain or host not allowed by this mail server.	From/To information

Understanding administrator notifications

Administrator email addresses for all alerts are configured on the Configuration menu on the Accounts tab.

Table 5-3 shows administrator notification information.

Table 5-3 Administrator notification information

Event	Default subject	Default message	Other information
Content violation	Content violation	Content violation found in email message.	■ From/To information ■ How message was handled (dropped, logged, or forwarded) ■ What content violation occurred (blocked because of message size or subject line)

Table 5-3 Administrator notification information

Event	Default subject	Default message	Other information
Spam **Note:** Notification is not sent when spam is detected by the heuristic spam engine.	Spam violation	Spam violation found in email message.	■ From/To information ■ Spam information ■ How message was handled (dropped, logged, or forwarded)

Understanding notification metatags

Within the default text of notifications there are metatags, which act as placeholders for information. You can change text in any notification, but do not alter the metatags, or you will not receive information about the event that triggered the notification.

Table 5-4 describes metatags and shows examples.

Table 5-4 Notification metatags

Metatag	Description	Example
MSGINFO	Tag in Content Violation notification to sender. Contains From/To information.	■ From: somebody@nnnn.com ■ To: someone@nnnn.com
DISPOSITION	Tag in Content Violation notification to administrator. Contains information about how the message was handled.	The message was dropped.
CONTENTINFO	Tag in Content Violation notification to administrator and sender. Contains content filter-specific data for the following: ■ Subject line blocked ■ Message too large	■ Subject: <specified by user> Matching Subject: <subject line matched>
SPAMINFO	Tag in Spam Violation notification to administrator. Contains spam-specific data such as the rule that was used to block a particular message.	■ From: <from address> ■ Matching list: <matching list>

Configuring notifications

You can configure Symantec AntiSpam for SMTP to send sender and administrator notifications when the following is detected:

- Content violation
- Anti-spam list violation

Notifications are configured on the Notify tabs in the product.

Note: Notification is not sent when spam is detected by the heuristic spam engine.

To configure notifications

1. On the appropriate Notify tab, check **Notify sender**, **Notify administrator**, or both.
2. If you selected to notify sender, under Notification for sender, either accept the default Subject and Message text or delete the default text and type your own.
3. If you selected to notify administrator, under Notification for administrator, either accept the default Subject and Message text or delete the default text and type your own.
4. Click **Save Changes**.

Note: Do not alter the metatags (for example, {$MSGINFO}). Metatags act as placeholders for information that will be included in notifications.

Generating reports

Symantec AntiSpam for SMTP generates two types of reports:

- Summary: Shows totals for message activity
  See “Generating summary reports” on page 64.
- Detail: Shows detailed information about message activity (to include dates of occurrences and client IP addresses, for example)
  See “Generating detail reports” on page 65.

Generating summary reports

The summary report lists totals for message processing.

To generate a summary report

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Reporting**.
2. On the Summary Report tab, in the From and To lists, select the date and time range for the report.
3. Click **Generate Report**.

See "About message summaries" on page 64.

When there is data logged for the following, there is an additional section of the report that displays:

- Subjects Blocked: Appears only when emails have been rejected due to blocked subject lines. It shows the subject line that triggered the block during the designated time period, a total for each blocked subject line, and a grand total.

About message summaries

Table 5-5 includes message summary information.

Table 5-5 Message summary information

Action	Description
Messages accepted	Number of messages that were added to the fast queue
Data accepted (KB)	Cumulative size of messages
Messages rejected	Number of messages that were rejected because the software is configured to reject messages, disallowed characters are in an email address, an anti-relay violation occurs, or the configured message size has been exceeded
Messages bounced	Number of incoming messages that were bounced
Messages delivered	Number of outgoing messages that were delivered
Message delivery failures	Number of outgoing messages that were returned due to delivery error
Messages completed	Number of messages that were processed by Symantec AntiSpam for SMTP

Generating detail reports

A detail report contains all of the events in the Symantec AntiSpam for SMTP log. You can configure Symantec AntiSpam for SMTP to log entries for various lengths of time.

See "Configuring logging options" on page 41.

You can save the report in a comma-delimited (CSV) text file for import into spreadsheets or other graphical display software. The CSV report is saved in the log directory that was specified at installation (by default, \Program Files\Symantec\SASSMTP\logs). The report file name is SASSMTPyyyymmddhhmm.CSV, which indicates the date and time of creation.

Note: There are legacy fields (Mailbox and Mailbox ID) that are in the CSV report that are no longer used and are always empty.

To generate a detail report

1. On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Reporting**.
2. On the Detail Report tab, in the From and To lists, specify the date and time range for the report.
3. Check the actions to include in the report.
4. In the Search box, you can type a single search term or string to narrow the output of the report.
   The search is not case sensitive.

   Note: If no actions are checked, the report contains all of the entries from the log.
5. Click **Generate Report** or **Write to CSV**.

The following are types of actions that can be included in a detail report:

- System: Associated with the operation of the Symantec AntiSpam for SMTP server
  See "About system actions" on page 66.
- SMTP: Associated with the transmission of mail between the server running Symantec AntiSpam for SMTP and other mail transfer agents (MTAs)
  See "About SMTP actions" on page 67.

- Message: Associated with email processing
  See "About message actions" on page 67.
- Blocking: Associated with blocking messages
  See "About blocking actions" on page 68.

About system actions

Table 5-6 shows the system actions.

Table 5-6 System actions

Action	Description
Logon	Shows the date and time of logon, the logon result (Succeeded/ Failed), the user who logged on, and the user's client IP address
Logoff	Shows the date and time of logoff, the logoff result (Succeeded/ Failed), the user who logged off, and the user's client IP address
Object modified	Shows the date that information was changed through the administrative interface, what was modified, which user modified it and from which client, and the type of modification that was made
Service started	Shows the date and time that the Symantec AntiSpam for SMTP service started
Service start failed	Shows the date and time that the Symantec AntiSpam for SMTP service failed to start
Service stopped	Shows the date and time that the Symantec AntiSpam for SMTP service stopped
Reordering started	Shows the date and time that queue reordering started
Reordering stopped	Shows the date and time that queue reordering stopped, the number of messages moved to the front of the queue, and the number of seconds spent performing a queue reorder

About SMTP actions

Table 5-7 shows the SMTP actions.

Table 5-7 SMTP actions

Action	Description
Connection from	Shows the date and time that any mail client attempts to connect to the Symantec AntiSpam for SMTP server, the result of the connection (Succeeded/Failed), the client’s IP address, and the connection ID
Connected to	Shows the date and time that Symantec AntiSpam for SMTP server attempts to connect to any mail server, result of the connection (Succeeded/Failed), connection ID, and connection information (Actual/Cached)
Disconnected	Shows which client or mail server was disconnected, the client ID, and the date and time of the disconnection
Connection closed	Shows the date and time that the connection was closed, IP address of the server connected to the Symantec AntiSpam for SMTP server, connection ID, last command sent, and last response sent by the disconnecting server
Protocol violation	Shows which client committed the violation, the connection ID, information about the protocol violation, and the date and time of the violation
Rejected	Shows that a message was rejected, which client it was rejected from, date and time of rejection, and reason for rejection

About message actions

Table 5-8 shows the message actions.

Table 5-8 Message actions

Action	Description
Accepted	Shows the date and time that a message was accepted, the From/To information, the subject, the client IP address, the connection ID, and the SMTP ID
Dropped	Shows the date and time that a message was dropped, From/To information, the reason for the drop, and the SMTP ID
Bounced	Shows the date and time that a message was bounced, To information, the reason for the bounce, and the SMTP ID

Table 5-8 Message actions

Action	Description
Delivered	Shows the date and time that a message was delivered, From/To information, the client IP address, the connection ID, and the SMTP ID
Delivery failed	Shows the date and time that a message was delivered and the SMTP ID
Completed	Shows the date and time that a message failed to be delivered, the client IP address, and the SMTP ID
Delivery suppressed	Shows the date and time that a message was not delivered, From/To information, and the SMTP ID

About blocking actions

Table 5-9 shows the blocking actions.

Table 5-9 Blocking actions

Action	Description
Subjects blocked	Shows the date that the subject was blocked, From information, subject, and which word or phrase was matched in the subject
Sender blocked	Shows the date and time of the block and the sender address
Spam list block	Shows the date and time of the block, how the message was handled, From/To information, SMTP ID, and the reason for the block
Spam detection	Shows the date and time of the heuristic spam detection, the client IP address, From/To information, subject, message size, SMTP ID, spam definitions date, and the spam probability score (percent certainty).

Integrating Symantec AntiSpam for SMTP with SESA

This chapter includes the following topics:

- About SESA
- Configuring logging to SESA
- Interpreting Symantec AntiSpam for SMTP events in SESA
- Uninstalling the SESA Integration Package
- Uninstalling the local SESA Agent

About SESA

In addition to using standard local logging for Symantec AntiSpam for SMTP, you can also choose to log events to the Symantec Enterprise Security Architecture (SESA). SESA is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control of security within an organization. It provides a common management framework for SESA-enabled security products, such as Symantec AntiSpam for SMTP, that protect your IT infrastructure from malicious code, intrusions, and blended threats.

SESA helps you increase your organization's security posture by simplifying the task of monitoring and managing the multitude of security-related events and products that exist in today's corporate environments. SESA includes an event management system that employs data collection services for events generated on computers that are managed by Symantec security products. The event categories and classes include antivirus, content filtering, network security, and systems management. The range of events varies depending on the Symantec applications that are installed and managed by SESA.

You can monitor and manage these security-related events through the SESA Console. The SESA Console is the common user interface that provides manageable integration of security technologies (Symantec or otherwise), Symantec Security Services, and Symantec Security Response. You can query, filter, and sort data to reduce the security-related events that you see through the SESA Console, which allows you to focus on threats that require your attention. You can configure alert notifications in response to events, and generate, save, and print tabular and graphical reports of event status, based on filtered views that you have created.

SESA is purchased and installed separately. SESA must be installed and working properly before you can configure Symantec AntiSpam for SMTP to log events to SESA.

For more information, see the SESA documentation.

Configuring logging to SESA

The logging of events to SESA is in addition to the standard local logging features for Symantec AntiSpam for SMTP. Logging to SESA is activated independently of standard local logging. If you have purchased SESA, you can choose to send a subset of the events logged by Symantec AntiSpam for SMTP to SESA.

See “Interpreting Symantec AntiSpam for SMTP events in SESA” on page 78.

To configure logging to SESA, you must complete the following steps:

- Configure SESA to recognize Symantec AntiSpam for SMTP. In order for SESA to receive events from Symantec AntiSpam for SMTP, you must run the SESA Integration Wizard that is specific to Symantec AntiSpam for SMTP on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the individual security product (in this case, Symantec AntiSpam for SMTP) to SESA.
  See “Configuring SESA to recognize Symantec AntiSpam for SMTP” on page 71.
- Install a local SESA Agent on the computer that is running Symantec AntiSpam for SMTP. The local SESA Agent handles the communication between Symantec AntiSpam for SMTP and SESA.
  See “Installing the local SESA Agent using the Agent Installer” on page 72.

- Configure Symantec AntiSpam for SMTP (through the administrative interface) to communicate with the local SESA Agent and to log events to SESA.

  See "Configuring Symantec AntiSpam for SMTP to log events to SESA" on page 77.

Configuring SESA to recognize Symantec AntiSpam for SMTP

To configure SESA to receive events from Symantec AntiSpam for SMTP, run the SESA Integration Wizard that is specific to Symantec AntiSpam for SMTP on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying Symantec AntiSpam for SMTP to SESA. You must run the SESA Integration Wizard for each SESA Manager computer to which you are forwarding events from Symantec AntiSpam for SMTP.

Each product that interfaces with SESA has a unique set of integration components. The integration components for all products that interface with SESA are available when you purchase SESA and are not distributed with the individual security products. Thus, the SESA integration component is not part of the Symantec AntiSpam for SMTP software distribution package.

See "Uninstalling the SESA Integration Package" on page 78.

To configure SESA to recognize Symantec AntiSpam for SMTP

1. On the computer on which the SESA Manager is installed, insert the Symantec Event Manager CD into the CD-ROM drive.
2. At the command prompt, change directories on the CD to \SASSMTP 3.1\Sesa.
3. At the command prompt, type:

   java -jar setup.jar

   The SESA Integration Wizard starts.
4. Click **Next** until you see the SESA Domain Administrator Information window.

5. In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you are using authenticated SSL instead of SESA default, anonymous SSL, you must enter the host name of the SESA Directory computer. For example, mycomputer.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
SSL Port	The number of the SESA Directory secure port. The default port number is 636.

6. Follow the on-screen instructions to install the appropriate SESA Integration Package and complete the SESA Integration Wizard.
7. Repeat steps 1 through 6 on each SESA Manager computer to which you are forwarding Symantec AntiSpam for SMTP events.

Installing the local SESA Agent using the Agent Installer

The local SESA Agent handles the communication between Symantec AntiSpam for SMTP and SESA and is installed on the same computer that is running Symantec AntiSpam for SMTP. The local SESA Agent is provided as part of the software distribution package for Symantec AntiSpam for SMTP. A separate installation package for installing the Agent, sesa_agent_installer, is located in the SESA_agent directory on the distribution CD for Symantec AntiSpam for SMTP.

If you have more than one SESA-enabled product installed on a single computer, these products can share a local SESA Agent. However, each product must register with the Agent. Thus, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must run the installer to register Symantec AntiSpam for SMTP.

The local SESA Agent is preconfigured to listen on IP address 127.0.0.1 and port number 8086. Symantec AntiSpam for SMTP uses this information to communicate with the Agent. If you must change the IP address or port number for the Agent, you must do so through the SESA Console. (Once an Agent is installed, it is controlled through the SESA Console, even though it is running on the same computer that is running the security product.) You must also update, through the Symantec AntiSpam for SMTP administrative interface, the information that Symantec AntiSpam for SMTP uses to contact the local SESA Agent.

For more information, see the SESA documentation.

See "Configuring Symantec AntiSpam for SMTP to log events to SESA" on page 77.

Install the SESA Agent using the Symantec AntiSpam for SMTP SESA Agent Installer

To install the SESA Agent using the SESA Agent Installer that Symantec AntiSpam for SMTP provides, run the Installer on all computers on which Symantec AntiSpam for SMTP 3.1 is installed.

See "Uninstalling the local SESA Agent" on page 79.

To install the SESA Agent on Windows 2000 Server/Advanced Server

1. Log on to the computer on which you have installed Symantec AntiSpam for SMTP as administrator or as a user with administrator rights.
2. Copy the executable (.exe) file to install the Agent from the Symantec AntiSpam for SMTP distribution CD onto the computer.
3. Run the .exe file.
4. Indicate that you agree with the terms of the Symantec license agreement, then click **Next**.
   If you indicate No, the installation is cancelled.
5. From the list of products to register with SESA, select Symantec AntiVirus for SMTP Gateways.
   You can register only one product at a time. If you are installing the SESA Agent to work with more than one Symantec product, you must run the installer again for each product.
6. Under Choose Destination Location, select the location in which to install the local Agent, then click **Next**.
   The default location is C:\Program Files\Symantec\SESA.
   If the SESA Agent is already installed on the same computer, this option does not display.

7. In the Primary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the primary SESA Manager is running.

   If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).

8. In the Primary SESA Manager port number box, type the port number on which the SESA Manager listens.

   The default port number is 443.

9. If you are running a Secondary SESA Manager that is to receive events from Symantec AntiSpam for SMTP, do the following:

   - In the Secondary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - In the Secondary SESA Manager port number box, type the port number on which the Secondary SESA Manager listens.

     The default port number is 443.

10. In the Organizational unit distinguished name box, type the organizational unit distinguished name to which the Agent will belong.

    If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:

    ou=Europe,ou=Locations,dc=SES,o=symc_ses

    The domains (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

11. Select one of the following:

    - Start SESA Agent Automatically: The SESA Agent starts automatically whenever the computer is restarted.
    - Start SESA Agent Manually: You must manually restart the SESA Agent each time that the computer is restarted.

12. Check **Check box here if you want the SESA Agent to start at installation completion** to have the SESA Agent start immediately after the installation finishes.

    If you do not check the check box, you must manually start the SESA Agent after the installation is complete.

The installer proceeds from this point with the installation. When the installation is complete, the Agent is installed as a Windows 2000 service, and is listed as SESA AgentStart Service in the Services Control Panel.

To install the SESA Agent on Solaris

1. Log on as root to the computer on which you have installed Symantec AntiSpam for SMTP.
2. Do one of the following:
   - Copy the shell (.sh) file to install the Agent from the Symantec AntiSpam for SMTP distribution CD onto the computer, and change directories to the location where you copied the file.
   - Run the Agent Installer file from the Symantec AntiSpam for SMTP distribution CD.
3. Type **sh ./sesa_agent_installer.sh**, then press **Enter**.
4. Indicate that you agree with the terms of the Symantec license agreement, then press **Enter**.

   If you indicate No, the installation is cancelled.
5. From the list of products to register with SESA, select Symantec AntiVirus for SMTP Gateways.

   You can register only one product at a time. If you are installing the Agent to work with more than one Symantec product, you must run the installer again for each product.
6. Select the location in which to install the SESA Agent, then click **Next**.

   The default location is /opt/Symantec/SESA.

   If the SESA Agent is already installed on the same computer, this option does not display.
7. Do one of the following:
   - Type the IP address or host name of the computer on which the primary SESA Manager is running.

     If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
   - Type the port number on which the SESA Manager listens.

     The default port number is 443.
8. If you are running a Secondary SESA Manager that is to receive events from Symantec AntiSpam for SMTP, do the following:
   - Type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - Type the port number on which the Secondary SESA Manager listens.

     The default port number is 443.

9 Type the organizational unit distinguished name to which the Agent will belong.
If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:
ou=Europe,ou=Locations,dc=SES,o=symc_ses
The domains (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

10 Type one of the following to indicate whether the SESA Agent should start automatically on system boot:

- y: The SESA Agent starts automatically on system boot.
- n: You must manually restart the SESA Agent after each system boot.

11 Type one of the following to indicate whether the SESA Agent should start immediately after the installation finishes:

- y: The SESA Agent starts immediately after installation.
- n: You must manually start the SESA Agent after installation.

The installer proceeds from this point with the installation. Unless you indicated otherwise during the installation, the SESA Agent starts automatically when the installation is complete. You may need to stop and restart the SESA Agent. A transcript of the installation is save as /var/log/SESAAGENT-install.log for later review.

Installing the SESA Agent manually by command line

As an alternative to using the SESA Agent Installer, you can install the SESA Agent by command line.

Install the SESA Agent manually by command line

To install the SESA Agent, you do the following:

- Prepare to install the SESA Agent.
- Install the SESA Agent by command line.

To prepare to install the SESA Agent

1 On the computer on which Symantec AntiSpam for SMTP is installed, create a folder for the SESA Agent files.
For example, C:\Agent.

2 Insert the SESA CD1 - SESA Manager into the CD-ROM drive.

3 Copy the files from the \Agent folder on the CD and paste them in the newly created folder on the Symantec AntiSpam for SMTP computer.

4 In a text editor, open the **Agent.settings** file.
For example, C:\Agent\Agent.settings.

5 Change the value of the mserverip setting to the IP address of the SESA Manager to which Symantec AntiSpam for SMTP will forward events.

6 Save and close the **Agent.settings** file.

To install the SESA Agent by command line

1 On the computer on which Symantec AntiSpam for SMTP is installed, at the command prompt, change to the folder in which the SESA Agent files reside.
For example, C:\Agent.

2 At the command prompt, type the following:
java -jar agentinst.jar -a3010
3010 is a unique product ID to install the Agent for Symantec AntiSpam for SMTP. To remove the SESA Agent, you must use the same product ID parameter (for Symantec AntiSpam for SMTP, 3010).
Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

Configuring Symantec AntiSpam for SMTP to log events to SESA

After you have installed the local SESA Agent to handle communication between Symantec AntiSpam for SMTP and SESA, you must configure Symantec AntiSpam for SMTP to communicate with the Agent by specifying the IP address and port number on which the Agent listens. You must also ensure that logging to SESA has been activated. These settings are located on the Symantec AntiSpam for SMTP administrative interface.

To configure Symantec AntiSpam for SMTP to log events to SESA

1 On the Symantec AntiSpam for SMTP administrative interface, in the left pane, click **Configuration**.

2 On the Logging tab, under SESA logging, check **Enable SESA logging**.

3 In the SESA agent host box, type the IP address on which the local SESA Agent listens.
The default setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.

4 In the Port number box, type the TCP/IP port number on which the local SESA Agent listens.

The port number you enter here must match the port number on which the local SESA Agent listens. The default port is 8086.

5 Click **Save Changes**.

Interpreting Symantec AntiSpam for SMTP events in SESA

SESA provides extensive event management capabilities, such as common logging of normalized event data for SESA-enabled security products like Symantec AntiSpam for SMTP. The event categories and classes include antivirus, content filtering, network security, and systems management. SESA also provides centralized reporting capabilities, including graphical reports. Currently, the events forwarded to SESA by Symantec AntiSpam for SMTP take advantage of the existing SESA infrastructure for events.

You can create alert notifications for certain events. Notifications include pagers, SNMP traps, email, and operating system event logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages.

For more information on interpreting events in SESA and on the event management capabilities of SESA, see the SESA documentation.

Uninstalling the SESA Integration Package

If Symantec AntiSpam for SMTP is no longer forwarding messages to SESA, you can uninstall the SESA Integration Package from each computer that is running the SESA Manager.

To uninstall the SESA Integration Package

1 On the taskbar, click **Start** > **Run**.

2 At the command prompt, type: **java -jar setup.jar -uninstall**

Uninstalling the local SESA Agent

The local SESA Agent is automatically uninstalled when you uninstall Symantec AntiSpam for SMTP. If more than one product is using the Agent, the uninstall script removes only the Symantec AntiSpam for SMTP registration and leaves the Agent in place. If no other security products are using the Agent, the uninstall script will uninstall the Agent as well.

Index

A

administrative interface 18
administrator settings 23
alerts, system 39

B

blocking, by message criteria 48

D

directories, installation 15
DNS 10, 13

H

hold queue 33
HTTP 17, 29
HTTPS 17, 30

I

installing
- SESA Agent 72
- Symantec AntiSpam for SMTP Gateways 12, 14

L

local SESA Agent, installing 72
logging
- configuring for SESA 69
- configuring for Symantec AntiSpam for SMTP 41

M

mail delivery 28

N

notifications 61

Q

queue file save 44

R

reports
- detail 65
- summary 64

routing
- default 34
- local 36

S

SESA Agent, installing for Symantec AntiSpam for SMTP Gateways 76
SESA Integration Wizard, installing 71
SESA, logging
- configuring 70
- configuring event logging 77

SESA, logging to
- installing the local Agent 72
- running the SESA Integration Wizard 71

SMTP 27
- conversation logging 45
- servers, conflicts with 11

spam
- blocking 49
- DNSBL anti-spam lists 51
- preventing relay 55
- white lists 53

status page 59
system requirements 11

U

uninstalling
- SESA Agent 79
- SESA Integration Package 78
- Symantec AntiSpam for SMTP Gateways 20